

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA

v.

ZACHARY SHAMES,

Defendant.

Case No. 16-CR-289

Hon. Liam O’Grady

Sentencing: January 26, 2018

POSITION OF THE UNITED STATES ON SENTENCING

Zachary Shames was a talented student at an affluent high school. He excelled at computer programming and earned admission to a private college to study computer science. But in his spare time he engaged in a years-long criminal scheme—one that lasted well into his college years. Shames designed a type of malicious software (or “malware”) called a keylogger and sold it online to over 3,000 people. Shames’s customers then used the keylogger for its intended purpose: to violate the privacy and security of over 16,000 innocent victims.

Shames’s keylogger made hacking easy. Its user-friendly interface allowed customers to check boxes to indicate what information they wanted to steal from the victim computers. The options ranged from passwords to the victim’s online accounts to every single keystroke typed on the victim’s computer. Shames’s keylogger would then produce a link that, if clicked by an unsuspecting victim, would give Shames’s hacker-clients access to the victim’s computer. Shames’s malware would then do what it was designed to do: steal the information requested and send it to an account designated by the hackers. To infect a victim and obtain this sensitive information, all Shames’s hacker-clients needed to do was trick a victim into clicking the link.

It is impossible to know the precise harms caused by the over 16,000 computer intrusions that Shames facilitated, but these types of intrusions serve two chief purposes: fraud and spying. The information that Shames allowed his clients to steal included sensitive financial information, such as online banking passwords, that could easily be used to empty a victim's bank account. And the non-financial uses of Shames's product are arguably even worse: Shames enabled his clients to gain access to victims' email, social media, and cloud storage accounts where many people store their most private information. In the hands of malevolent actors, such information could be used to embarrass, to harass, and to blackmail.

Malware developers like Shames are the root cause of computer hacking. Many hackers do not have the technical ability to create the malware they use to hack computers; just as the overwhelming majority of people who use any other type of software do not have ability to build the software themselves. Shames and other malware developers like him exponentially increase the number of actors with the ability to engage in computer hacking. That is why people who create malware and distribute it widely over the internet have been and continue to be a major priority for the law enforcement agencies who are charged with protecting the public from computer hacking.

Given these grave concerns, the government would normally recommend a sentence within its recommended guidelines range of 57 to 71 months' imprisonment. But the government has moved to reduce that range by 50% under U.S.S.G. § 5K1.1, and therefore recommends a sentence within the resulting range of **28 to 35 months**.

I. Offense of Conviction

From January 2012 through December 2014, Shames developed, marketed, sold, and supported computer keylogging software (hereinafter, the “Keylogger”). PSR ¶ 14. Shames designed the Keylogger for the purpose of allowing users to access victim computers without authorization and steal information. PSR ¶ 17. In particular, the Keylogger could record everything typed into the infected computers—all “keystrokes”—and send reports of those keystrokes to the hacker who controlled the Keylogger. PSR ¶ 15. It could also steal the usernames and passwords of any online account—including email, banking, and social media accounts—that a victim saved on his or her browser. *Id.* Shames even gave his customers the ability to take “snapshots” of whatever was on their victims’ computer screens. *Id.* To infect more computers, the Keylogger allowed users to access their victims’ contact lists and send custom messages to the victims’ friends and family pretending to be the victim and inviting the victim’s friends to click a link that would infect the friend’s computer. *Id.* In total, Shames’ Keylogger generated over of 4 million of key log reports (or “logs”) that transferred private information from the 16,000 victim computers to Shames’s clients. PSR ¶ 29.

Shames knew that his customers were using these features to steal sensitive information from their victims and that this information could be used to commit fraud or to spy on the victims. PSR ¶ 17. He marketed and sold the Keylogger on a hacking website. PSR ¶ 16. He posted a video on YouTube in which he instructed customers step-by-step in how to use his Keylogger to spy on victims (“victims” is a word Shames used repeatedly in the video to refer to computers infected by his Keylogger). PSR ¶ 24. Shames provided repeated support to his customers over email and on the hacking website on which he sold the Keylogger. PSR ¶¶ 19-23. During these conversations, Shames touted his Keyloggers’ ability to steal email and social media passwords,

id., and agreed to build a custom keylogger (for an increased price) for a customer who declared that he wanted “to record all keystrokes and recover all passwords.” PSR ¶ 21.

Based on these facts, Shames pled guilty in this Court to aiding and abetting computer intrusions, in violation of 18 U.S.C. § 1030(a)(5)(A). PSR ¶ 1-2. The maximum penalty for this offense is 10 years’ imprisonment, a \$250,000 fine, and 3 years’ supervised release. PSR ¶ 72.

II. Guidelines Range

A. Calculation By Probation Officer

The probation officer calculated the defendant’s offense level as follows:

| Guideline | Offense Level |
|--|---------------|
| Base Offense Level (U.S.S.G § 2B1.1(a)(1)) | 6 |
| Loss amount between \$550,000 but less than \$1.5 million (U.S.S.G § 2B1.1(b)(1)(H)) | +14 |
| Offense involved 10 or more victims (U.S.S.G § 2B1.1(b)(2)(A)) | +2 |
| The defendant was convicted of an offense under 18 U.S.C. § 1030, and the offense involved an intent to obtain personal information. (U.S.S.G § 2B1.1(b)(17)(A)) | +2 |
| The defendant was convicted of an offense under 18 U.S.C. § 1030(a)(5)(A). (U.S.S.G § 2B1.1(b)(18)(A)(ii)) | +4 |
| The defendant used a special skill, in a manner that significantly facilitated the commission or concealment of the offense. (U.S.S.G § 3B1.3) | +2 |
| Acceptance of responsibility (Section 3E1.1) ¹ | -3 |
| TOTAL | 27 |

PSR ¶¶ 34-46. The government is not seeking an enhancement under U.S.S.G § 2B1.1(b)(17)(A) for an intent to obtain personal information. Therefore, considering the defendant’s Category I criminal history, the resulting guidelines range (before considering the government’s motion under

¹ The Government hereby moves, under U.S.S.G. § 3E1.1(b), for a third point to be reduced from the defendant’s offense level, based on the defendant’s timely acceptance of responsibility.

U.S. Sentencing Guideline 5K1.1) is 57-71 months' imprisonment. *Id.* ¶¶ 73-75.

B. Enhancement for Loss Amount

The parties have stipulated, and the probation officer has agreed, that a fourteen-point enhancement is appropriate under U.S.S.G. § 2B1.1(b)(1)(H) because the loss attributable to the defendant exceeded \$550,000 but was less than \$1.5 million. In particular, the parties have agreed that \$606,400 is a reasonable estimate of the loss attributable to Shames. PSR ¶ 27. The parties calculated this loss as follows. First, they agreed that Shames should not be held responsible for computer intrusions committed by people who purchased the Keylogger from Shames before Shames's eighteenth birthday (which was in August 2013). While all 16,847 intrusions included in the presentence report occurred after Shames turned eighteen, the government was able to estimate that approximately 3,032 of them were committed with versions of the Keylogger that Shames sold after his eighteenth birthday. PSR ¶ 27. The government then estimated that the reasonable costs to repair a computer infected with this particular type of malware was \$200.00. *Id.* This figure is based on information the FBI received from four private computer service companies that offer malware remediation services. *Id.* The estimate includes the cost of backing up personal files from the infected computer, wiping the computer's hard drive, and then reinstalling the computer's operating system. *Id.* Consideration of such costs is appropriate under the guidelines, which counsel that loss amount for computer intrusions should include "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense." U.S.S.G. § 2B1.1, note 3(A)(v)(III); *accord* 18 U.S.C. § 1030(e)(11). Accordingly, the parties reached the loss figure of \$606,400 by multiplying the number of computers infected with

versions of the Keylogger that Shames sold after his eighteenth birthday (3,032) by the cost of repairing those computers (\$200).

C. Enhancement for Use of a Special Skill

The probation officer appropriately recommends a two-point enhancement because Shames “used a special skill ... in a manner that significantly facilitated the commission or concealment of the offense.” U.S.S.G. § 3B1.3. “‘Special skill’ refers to a skill not possessed by members of the general public and usually requires substantial education, training, or licensing.” U.S.S.G. § 3B1.3 note 4. Courts have repeatedly held that a special skill enhancement is appropriate where, as here, the defendant has knowledge of computers that far exceeds that of the general public and uses that knowledge to commit the crime. *See United States v. O'Brien*, 435 F.3d 36, 42 (1st Cir. 2006) (upholding special skill enhancement for defendant who worked as a computer consultant was thus “plausibly found to have had such skills beyond those possessed by an ordinary computer user”); *United States v. Petersen*, 98 F.3d 502, 506 (9th Cir. 1996) (upholding special skill enhancement for defendant who had no “formal training in computers” and who did not have the ability to “create [computer] programs,” but who “obviously has an extraordinary knowledge of how computers work”).

Like the defendants in *O'Brien* and *Petersen*, Shames obviously has “substantial knowledge in software development,” PSR ¶ 30, as found by probation. By the time the offense ended in December 2014, Shames was a sophomore computer science major at a prestigious university and had spent the prior summer employed by a technology company. PSR ¶¶ 30, 66. More importantly, Shames’s skills in computer programing are evident from the fact that as a high school student he was able code one of the most popular keyloggers on the internet. Indeed, in 2014, one

of Shames's clients gushed that Shames's keylogger "is still the best" available and that, while the customer had purchased competing products, he had "more trust" in Shames's product. PSR ¶ 20.

The defense has argued that a special skill enhancement is inappropriate because Shames did not have a professional license and his software development skills were largely self-taught. But computer programmers are often self-taught; indeed, Silicon Valley is littered with the success stories of self-taught programmers. That is why courts have rightly rejected the argument that one cannot have special computer skills without formal training or a license. *See Petersen*, 98 F.3d at 507 ("substantial education, training or licensing ... is not an absolute prerequisite for a special skill adjustment. Despite Petersen's lack of formal training or licensing, his sophisticated computer skills reasonably can be equated to the skills possessed by pilots, lawyers, chemists, and demolition experts for purposes of § 3B1.3"); *United States v. Malgoza*, 2 F.3d 1107, 1111 (11th Cir.1993) (defendant's advanced level of radio operating ability constitutes a special skill).

The defense has also argued that applying the special skill enhancement here would amount to double-counting because specialized computer skills are inherent in every § 1030 violation. Not true. There are plenty of ways to commit a § 1030 violation, or to aid and abet such a violation, without possessing or employing special skills. One with no special knowledge of computers could, for instance, obtain another's computer password through a business or personal relationship and use that password to commit unauthorized computer intrusions or to aid others in the same. *See O'Brien*, 435 F.3d at 42 ("special computer skills is certainly not an element [a § 1030] offense"). Indeed, the whole point of Shames's Keylogger was to allow people without particularly good computer skills to engage in hacking. Instead, Shames's clients could rely on Shames to supply the necessary computer programming skills. The very fact that 3,000 people were

willing to pay Shames for his computer programming skills shows that he has a skill “not possessed by members of the general public.” U.S.S.G. § 3B1.3 note 4. And the skill with which Shames developed this product surely “magnifie[d] or facilitate[d] the potential for harm.” *O’Brien*, 435 F.3d at 42.

III. Sentencing Recommendation

As the Court is well aware, the Sentencing Guidelines are advisory, and just one factor that must be considered along with the other factors set forth in 18 U.S.C. § 3553(a).² The government recommends a sentence within the adjusted guidelines range of **28-35 months’ imprisonment**, and believes that such a sentence is supported by other § 3553(a) factors, particularly the need for a sentence that reflects the seriousness of the offense and adequately deters others from perpetrating similar crimes. However, the government does agree that the defendant’s age is also a factor that should be considered and thus agrees that the Court’s consideration of Sentencing Guideline 5H1.1 is warranted.

A. The Sentence Should Reflect Shames’s Role in Invading the Privacy and Endangering the Data Security of Thousands of People.

It is difficult to calculate the full harm caused by Shames’s Keylogger. We know that his Keylogger allowed his customers access to the private information of over 16,000 innocent victims

² The § 3553(a) factors include: the nature and circumstances of the offense and the history and characteristics of the defendant; the need for the sentence imposed to reflect the seriousness of the offense, to promote respect for the law, to provide just punishment for the offense, to afford adequate deterrence to criminal conduct, to protect the public from further crimes of the defendant, and to provide the defendant with needed training, medical care, or other treatment; the kinds of sentences available; the kinds of sentence and the sentencing range established for the type of offense committed; any pertinent policy statement; the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct; and the need to provide restitution to any victims of the offense.

without their consent. This included some extremely sensitive information such as email and banking passwords and the content of any message the victim typed while his/her computer was infected. The government does not know exactly what Shames's customers did with the passwords they stole from their victims, but the privacy and security concerns associated with a malicious actor gaining access to one's email account is obvious. The defense will no doubt characterize these dangers as speculative, but stealing passwords was a central purpose of the Keylogger that Shames built and his communications with his customers make plain that he understood that his customers intended to use his Keylogger to access their victims email accounts without their consent. *See, e.g.*, PSR ¶ 23. Shames unleashed this malicious tool onto the public for his own profit despite knowing the clear dangers it posed to innocent people.

B. The Sentence Should Be Sufficient to Deter Other Malware Developers.

In the cybercrime world, malware developers are at the heart of the problem. They provide the technical expertise that others use to victimize the public. Like the defendant, they often sell their products online using a pseudonym and are thus able to make a lot of money from the comfort and anonymity of their living rooms. Like the defendant, these criminals often operate with impunity for years and begin to feel invincible. Unfortunately, high rewards and relatively low risk of detection are basic features of cybercrime that are not going to change anytime soon. The only way to affect the cost-benefit analysis of these crimes is to impose meaningful sentences on those who are caught. If the Court does so, there is every reason to believe that many would-be criminals will get the message. Computer hackers are among the most sophisticated criminals in the world and are known to closely monitor the government's response to cybercrime and plan accordingly. Achieving general deterrence in this area therefore appears particularly promising. *See United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006) (Because "economic and fraud-

based crime are more rational, cool, and calculated than sudden crimes of passion or opportunity, these crimes are prime candidates for general deterrence”).

IV. Conclusion

The government respectfully recommends a sentence within the adjusted guidelines range of **28 to 35 months’ imprisonment**, as well as an agreed-upon forfeiture order of \$60,993.00, and a fine. The guidelines state that “the court shall impose a fine in all cases, except where the defendant establishes that he is unable to pay and is not likely to become able to pay any fine.” U.S.S.G. § 5E1.2(a). Probation has determined that, even considering the forfeiture order, the defendant has the ability to pay at least a nominal fine, and that finding is well-supported by his financial disclosures. PSR ¶¶ 68-70. Accordingly, the government recommends a fine within the guidelines range of \$15,000 to \$150,000. PSR ¶ 72.

Dana J. Boente
United States Attorney

By: /s/
Kellen S. Dwyer
Assistant United States Attorney
United States Attorney’s Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, Virginia 22314
(703) 299-3700
kellen.dwyer@usdoj.gov

Catherine Alden Pelker, Trial Attorney
U.S. Department of Justice, Criminal Division
Computer Crime & Intellectual Property Section

January 19, 2018

Certificate of Service

I hereby certify that on January 19, 2018, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of filing (NEF) to counsel of record for the defense.

I also certify that on January 19, 2018, I will send a true and correct copy of the foregoing by e-mail to the following:

Karen M. Riffle
United States Probation Officer
Karen_Riffle@vaep.uscourts.gov

By: /s/
Kellen S. Dwyer
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, Virginia 22314
(703) 299-3700
kellen.dwyer@usdoj.gov